WAGNER BLECHER LLP
123 Westridge Drive
Watsonville, CA 95076
(408) 377-0500

PATENT APPLICATION

ATTORNEY DOCKET NO. TRMB-T11702

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Rodric FAN et al.

Confirmation No.: 6041

Application No.: 09/927,928

Examiner: Tamara TESLOVICH

Filing Date: 08/09/2001

Group Art Unit: 2437

Title: WIRELESS DEVICE TO NETWORK SERVER ENCRYPTION

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 10/25/2010 .

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $540.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $130	☐ 2nd Month $490	☐ 3rd Month $1110	☐ 4th Month $1730

☐ The extension fee has already been filed in this application.

☑ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge Dep. Acct. 50-4157 the sum of $ 540 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 50-4157 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 50-4157 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☑ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300 or via electronic transmission.
Date of facsimile/transmission: 12/20/2010
Typed Name: Brenda Dinapoli
Signature: /Brenda Dinapoli/

Respectfully submitted,
Rodric FAN et al.

By /John P. Wagner, Jr./

John P. Wagner, Jr.
Attorney/Agent for Applicant(s)
Reg No. : 35,398
Date : 12/20/2010
Telephone : 408-377-0500

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Fan et al.	Patent Application	
Serial No.:	09/927,928	Group Art Unit:	2437
Filed:	August 9, 2001	Examiner:	Teslovich, T.

For: WIRELESS DEVICE TO NETWORK SERVER ENCRYPTION

Appeal Brief

Table of Contents

I. Real Party in Interest

The assignee of the present embodiments is Trimble Navigation Limited.

II. Related Appeals and Interferences

There are no related appeals or interferences known to the Appellants.

III. Status of Claims

Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are pending. Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are rejected. Claims 5, 7, 8, 12-15, 18, 19, 21-24, 28 and 34 are canceled. This Appeal involves Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35.

IV. Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

V. Summary of Claimed Subject Matter

Claim 1 pertains to a method of transmitting secured data (page 2, lines 20-25). The method includes:

utilizing a first key to encrypt a payload by a mobile device (page 11, lines 16-17; 610 of Fig. 6);

adding a header to the encrypted payload to form a data packet by the mobile device (Fig. 5B; page 11, lines 17-18; 612 of Fig. 6), wherein the payload comprises GPS location of the mobile device (page 4, lines 20-26; page 11, lines 12-13);

utilizing a second key to encrypt the first key by the mobile device (page 7, lines 25-26; 608 of Fig. 6; page 12, lines 18-20);

utilizing a third key to encrypt the data packet by said mobile device (Fig. 5C; page 11, lines 23-25);

transmitting the encrypted first key separate from the encrypted data packet to a wireline device in a first transmission from the mobile device (page 8, lines 1-3; page 12, lines 21-25), wherein the wireline device decrypts the encrypted first key (page 8, lines 6-7);

transmitting only the encrypted data packet without the first key over a wireless link to a gateway in a second transmission from the mobile device (page 11, lines 25-30; block 616 of Fig. 6; page 14, lines 4-5), wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header (page 10, lines 5-6), and forwards the encrypted payload and the header to the wireline device over an open network (page 10, lines 7-8); and

utilizing the wireline device and the first key from the first transmission to

decrypt the encrypted payload (page 12, lines 6-9).

Claim 6 pertains to a device for transmitting secured data over a wireless link. The device includes:

an encryption engine which generates a first key (606 of Fig. 6; page 12, lines 18-20), encrypts a payload according to the first key (610 of Fig. 6; page 13, lines 22-23) adds a header to the encrypted payload to form a data packet (612 of Fig. 6; page 13, lines 29-30), encrypts the first key according to a second key (608 of Fig. 6; page 12, lines 18-20), and encrypts the data packet according to a third key (Fig. 5C; page 11, lines 23-25), wherein the payload comprises GPS location information obtained by the device and regarding a geographical location of the device (page 4, lines 20-26; page 11, lines 12-13); and

a wireless transceiver coupled to the encryption engine (Fig. 2; page 6, lines 16-22), the wireless transceiver transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from the device (page 8, lines 1-3; page 12, lines 21-25) and transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the device (block 616 of Fig. 6; page 14, lines 4-5), wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header (page 10, lines 5-6), and forwards the encrypted payload and the header to the server over an open network (page 10, lines 7-8);

wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload of the second transmission using the decrypted first key (page 12, lines 6-9).

Claim 10 pertains to a method for secured communication between a mobile device and a server on a wide area network. The method includes:

encrypting a payload at the mobile device using a first session key (block 610 of Fig. 6; page 13, lines 22-24), wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device (page 4, lines 20-26; page 11, lines 12-13);

encrypting the first session key at the mobile device using a public key (page 7, lines 25-26; 608 of Fig. 6; page 12, lines 18-20);

transmitting the encrypted first session key separate from an encrypted data packet to the server over a wireless link in a first transmission from the mobile device (page 8, lines 1-3; page 12, lines 21-25);

decrypting the encrypted first session key at the server (page 13, lines 9-14);

adding a header to the encrypted payload to form a data packet at the mobile device (Fig. 5B; page 11, lines 17-18);

encrypting the data packet according to a second session key configured for secured communications over the wireless link (Fig. 5C; page 11, lines 22-30); and

transmitting only the encrypted data packet without said first key in a second transmission from the mobile device to a gateway which decrypts the encrypted data packet to recreate the encrypted payload and the header (page 11, lines 25-30; block 616 of Fig. 6; page 14, lines 4-5), and forwards the encrypted payload and the header to the server (page 10, lines 7-8);

wherein the server utilizes the decrypted first session key, decrypted from the first transmission, to decrypt the encrypted payload (page 9, line 27 – page 10, line 3).

Claim 29 pertains to a computer readable storage medium comprising program instructions for performing a method including:

encrypting a payload according to a first key (block 610 of Fig. 6; page 13, lines 22-24), wherein said payload comprises GPS location of a mobile device (page 4, lines 20-26; page 11, lines 12-13);

adding a header to the encrypted payload to form a data packet (Fig. 5B; page 11, lines 17-18);

encrypting the first key according to a second key (608 of Fig. 6; page 12, lines 18-20);

encrypting the data packet according to a third key configured for secured communications over a wireless link (Fig. 5C; page 11, lines 23-25);

transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from said mobile device (page 8, lines 1-3; page 12, lines 21-25); and

transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the mobile device (block 616 of Fig. 6; page 14, lines 4-5), wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header (page 10, lines 5-6, and forwards the encrypted payload and the header to the server (page 10, lines 6-7), and wherein the server decrypts the encrypted first key received in the

first transmission and decrypts the encrypted payload using the decrypted first key (page 9, line 27 – page 10, line 3)..

VI. Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al. (US 6,055,314), hereinafter referenced as "Spies," in view of Inoue et al. (US 6,501,767) hereinafter referenced as "Inoue".

VII. Arguments

1. Whether Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are patentable over the combination of Spies and Inoue.

The instant Office Action states that Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Spies and Inoue. Appellants respectfully submit that Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are patentable over the combination of Spies and Inoue for at least the following rationale.

Claim 1 recites (emphasis added):

A method of transmitting secured data, the method comprising:
utilizing a first key to **encrypt a payload by a mobile device**;
adding a header to the encrypted payload to form a data packet by said mobile device, wherein said payload comprises **GPS location** of said mobile device;
utilizing a second key to encrypt the first key by said mobile device;
utilizing a third key to encrypt the data packet by said mobile device;
transmitting the encrypted first key separate from the encrypted data packet to a wireline device in a first transmission from said mobile device, wherein the wireline device decrypts the encrypted first key;
transmitting only the encrypted data packet without said first key over a wireless link to a gateway in a second transmission from said mobile device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network; and
utilizing the wireline device and the first key from the first transmission to decrypt the encrypted payload.

Independent Claims 6, 10 and 29 recite similar embodiments. Claims 2-4, 9, 11, 16, 17, 20, 25, 26, 30-33 and 35 that depend from Claims 1, 6, 10 and 29 respectively, also include these embodiments.

"As reiterated by the Supreme Court in *KSR*, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious" (emphasis in original; MPEP 2141.02(I)). Appellants note that "[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art" (emphasis added; MPEP 2141(III)).

Moreover, Appellants respectfully note that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention" (emphasis in original; MPEP 2141.02(VI); *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)).

First, Appellants respectfully submit that Spies does not teach or suggest "utilizing a first key to encrypt a payload by a mobile device," as claimed (emphasis added). Appellants respectfully submit that Spies teaches away from "utilizing a first key to encrypt a payload by a mobile device," as claimed (emphasis added). Appellants understand Spies to disclose a non-mobile device, at the location of a video content provider, that encrypts a payload. In particular, Spies discloses "a video content provider 22 includes a cable operator, a television station, and a movie studio" (col. 4, lines 65-66; emphasis added). In regards to the non-mobile device, Spies discloses "[a] video encryption device **at** the video content provider supplies a video data stream in encrypted format on a digital video disk" (col. 3, lines 42-45; emphasis added), and "[t]he provide computing unit 34 might be configured as a continuous media server that transmits video programs over a distribution network…or a reproduction mechanism that transfers video content programs onto portable media for mass distribution (e.g., digital video disks)" (col. 5, lines 25-33).

Accordingly, by disclosing (1) a continuous media server or (2) a reproduction mechanism that transfers video content programs onto DVD's that remain stationary at the location of a cable operator, television station or a movie studio, Appellants respectfully submit that Spies teaches away from "utilizing a first key to encrypt a payload by a mobile device," as claimed (emphasis added). Also, Appellants agree with the instant Office Action that states "Spies fails to particularly disclose wherein the device is a mobile device" (page 5.)

Second, Appellants respectfully submit that the combination of Spies and Inoue would render Spies unsatisfactory for its intended purpose. Appellants understand an intended purpose of Spies is to encrypt video data at the video content provider (e.g., cable operator, television station or a movie studio) by a stationary provider computing unit (e.g., server or reproduction mechanism that transfers video content programs onto DVD's). Appellants understand Inoue to disclose mobile devices "moving over different address spaces" (abstract). In particular, Inoue discloses "a user carries along a portable computer terminal and makes communications while moving over networks" (col. 1, lines 43-44). Accordingly, combining Spies and Inoue would modify a non-mobile server or reproduction mechanism located at a video content provider to a mobile server or reproduction mechanism that are carried around over different address spaces, such as away from the video content provider. Therefore, Appellants respectfully submit that the combination of Spies and Inoue would render Spies unsatisfactory for its intended purpose.

Third, Appellants respectfully submit that the combination of Spies and Inoue would change the principal operation of Spies. Appellants understand a principal operation of Spies is to encrypt video data at the video content provider (e.g., cable operator, television station or a movie studio) by a stationary provider computing unit (e.g., server or reproduction mechanism that transfers video content programs onto DVD's). Appellants understand Inoue to disclose mobile devices "moving over different address spaces" (abstract). In particular, Inoue

discloses "a user carries along a portable computer terminal and makes communications while moving over networks" (col. 1, lines 43-44). Accordingly, combining Spies and Inoue would change the principal operation of Spies to a mobile server or reproduction mechanism that are carried around over different address spaces, such as away from the video content provider. Therefore, Appellants respectfully submit that the combination of Spies and Inoue would change the principal operation of Spies.

Fourth, Appellants respectfully submit that Spies does not teach or suggest and is silent in regards to "said payload comprises GPS location of said mobile device," as claimed (emphasis added). Appellants understand Spies to disclose a video payload. In particular, Spies discloses "Fig. 4 shows packet P_i…[i]t contains security header 72 and a video data payload 74" (col. 9, lines 52-53). Accordingly, Appellants respectfully submit that Spies does not teach or suggest and is silent in regards to "said payload comprises GPS location of said mobile device," as claimed (emphasis added).

Moreover, Inoue does not overcome the deficiencies of Spies. Appellants understand Inoue to teach or suggest "[a] packet relay device for relaying packets having an address of the mobile computer device as a destination or source is provided at a border between a private address space and a global address space" (abstract, emphasis added). Moreover, Appellants do not understand a global address space to disclose a global positioning system (GPS)

location. Inoue does not teach or suggest "said payload comprises GPS location of said mobile device," as claimed (emphasis added).

Appellants respectfully submit that the combination of Spies and Inoue, as a whole, does not satisfy a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, Appellants respectfully submit that Claims 1, 6, 10 and 29 are in a condition for allowance. Appellants respectfully submit that the combination of Spies and Inoue also does not render obvious the additional claimed features as recited in Claims 2-4, 9, 11, 16, 17, 20, 25, 26, 30-33 and 35 that depend from Claims 1, 6, 10 and 29, respectively. Therefore, Claims 2-4, 9, 11, 16, 17, 20, 25, 26, 30-33 and 35 are in a condition for allowance as being dependent on an allowable base claim.

Conclusion

Appellants believe that pending Claims 1, 2, 4-16 and 18-21 are patentable over the asserted art.

Accordingly, Appellants respectfully submit that the rejections of Claims 1-4, 6, 9-11, 16, 17, 20, 25, 29-33 and 35 are improper and should be reversed.

Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: December 20, 2010

/John P. Wagner, Jr./
John P. Wagner, Jr.
Registration Number: 35,398

WAGNER BLECHER LLP
Westridge Business Park
123 Westridge Drive
Watsonville, CA 95076
408-377-0500

VIII. Appendix - Clean Copy of Claims on Appeal

1. A method of transmitting secured data, the method comprising:

utilizing a first key to encrypt a payload by a mobile device;

adding a header to the encrypted payload to form a data packet by said mobile device, wherein said payload comprises GPS location of said mobile device;

utilizing a second key to encrypt the first key by said mobile device;

utilizing a third key to encrypt the data packet by said mobile device;

transmitting the encrypted first key separate from the encrypted data packet to a wireline device in a first transmission from said mobile device, wherein the wireline device decrypts the encrypted first key;

transmitting only the encrypted data packet without said first key over a wireless link to a gateway in a second transmission from said mobile device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network; and

utilizing the wireline device and the first key from the first transmission to decrypt the encrypted payload.

2. The method of claim 1, wherein the first key comprises a symmetric key.

3. The method of claim 1, further comprising:

transmitting the encrypted first key to the wireline device, wherein the wireline device decrypts the encrypted first key using a private key associated with the second key.

4. The method of claim 1, wherein the third key comprises a symmetric session key.

6. A device for transmitting secured data over a wireless link, the device comprising:

an encryption engine which generates a first key, encrypts a payload according to the first key, adds a header to the encrypted payload to form a data packet, encrypts the first key according to a second key, and encrypts the data packet according to a third key, wherein the payload comprises GPS location information obtained by the device and regarding a geographical location of the device; and

a wireless transceiver coupled to the encryption engine, the wireless transceiver transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from the device and transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server over an open network;

wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload of the second transmission using the decrypted first key.

9. The device of claim 6, wherein the first key comprises a symmetric key.

10. A method for secured communication between a mobile device and a server on a wide area network, the method comprising:

encrypting a payload at the mobile device using a first session key, wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device;
encrypting the first session key at the mobile device using a public key;

transmitting the encrypted first session key separate from an encrypted data packet to the server over a wireless link in a first transmission from the mobile device;

decrypting the encrypted first session key at the server;

adding a header to the encrypted payload to form a data packet at the mobile device;

encrypting the data packet according to a second session key configured for secured communications over the wireless link; and

transmitting only the encrypted data packet without said first key in a second transmission from the mobile device to a gateway which decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server;

wherein the server utilizes the decrypted first session key, decrypted from the first transmission, to decrypt the encrypted payload.

11. The method of claim 10 wherein the decrypting the encrypted first session key at the server further comprises:

decrypting the encrypted first session key at the server using a private key associated with the public key.

16. The method of claim 10, further comprising:

generating the first session key at the mobile device based on a random number.

17. The method of claim 10, wherein the encrypting the payload at the mobile device using the first session key further comprises:

encrypting the payload at the mobile device using the first session key, wherein the first session key employs an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES.

20. The method of claim 1, further comprising:

implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES.

25. The method of claim 1, wherein the data packet includes GPS location information obtained by the wireless device and associated with a geographical location of the wireless device.

26. The method of claim 1, further comprising:

utilizing a random number to generate the first key.

27. The device of claim 6, further comprising:

a memory coupled to the encryption engine, wherein the memory stores the second key, and wherein the encryption engine accesses the second key from the memory.

29. A computer readable storage medium comprising program instructions for performing a method comprising:

encrypting a payload according to a first key, wherein said payload comprises GPS location of a mobile device;

adding a header to the encrypted payload to form a data packet;

encrypting the first key according to a second key;

encrypting the data packet according to a third key configured for secured communications over a wireless link;

transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from said mobile device; and

transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the mobile device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server, and wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload using the decrypted first key.

30. The computer readable storage medium of claim 29, wherein the first key

comprises a symmetric key.

31. The computer readable storage medium of claim 29, wherein the method further comprises:

receiving the data packet at the gateway;

decrypting the data packet at the gateway according to the third key;

forwarding the encrypted payload to the server;

receiving the encrypted first key at the server;

decrypting the encrypted first key using a fourth key; and

decrypting the payload according to the decrypted first key.

32. The computer readable storage medium of claim 29, wherein the first key comprises a symmetric session key.

33. The computer readable storage medium of claim 29, wherein the method further comprises:

implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES.

35. The computer readable storage medium of claim 32, wherein the symmetric session key is generated based on a random number.

IX. Evidence Appendix

No evidence is herein appended.

X. Related Proceedings Appendix

No related proceedings.